# ASA 8.2:使用ASDM通過nat、global、static和 access-list命令進行埠重定向(轉發)

## 目錄

簡介 必要條件 需求 採用元件 慣例 網路圖表 允許出站訪問 允許內部主機通過NAT訪問外部網路 允許內部主機通過PAT訪問外部網路 限制內部主機訪問外部網路 允許具有相同安全級別的介面之間的流量 <u>允許不受信任的主機訪問受信任網路中的主機</u> 禁用特定主機/網路的NAT <u>連線埠重新導向(轉送)(含靜態)</u> 使用靜態限制TCP/UDP會話 時間型存取清單 相關資訊

# <u>簡介</u>

本檔案介紹使用ASDM在思科調適型安全裝置(ASA)上執行連線埠重新導向的方式。它處理通過 ASA的流量的訪問控制以及轉換規則的工作方式。

# <u>必要條件</u>

## <u>需求</u>

思科建議您瞭解以下主題:

- <u>NAT概述</u>
- <u>PIX/ASA 7.X:連線埠重新導向</u>

## <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco 5500系列ASA版本8.2
- Cisco ASDM版本6.3

注意:此配置僅在Cisco ASA軟體版本8.0到8.2之間運行良好,因為NAT功能沒有重大更改。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

### <u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>



此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

# <u>允許出站訪問</u>

出站訪問描述從較高安全級別介面到較低安全級別介面的連線。這包括從內部到外部、從內部到非 軍事區(DMZ)以及從非軍事區到外部的連線。只要連線源介面的安全級別高於目標介面,這還可以 包括從一個DMZ到另一個DMZ的連線。

沒有配置轉換規則,任何連線都無法通過安全裝置。此功能稱為<u>nat-control</u>。此處顯示的影象說明 了如何通過ASDM禁用此功能,以便允許通過ASA的連線而無需任何地址轉換。但是,如果您配置 了任何轉換規則,則禁用此功能不會對所有流量保持有效,您需要明確排除網路的地址轉換。

## <u>允許內部主機通過NAT訪問外部網路</u>

您可以通過配置動態NAT規則來允許一組內部主機/網路訪問外部世界。為此,您需要選擇要授予訪問許可權的主機/網路的實際地址,然後必須將其對映到已轉換的IP地址池。

完成以下步驟,以允許內部主機通過NAT訪問外部網路:

1. 轉至Configuration > **Firewall** > **NAT Rules**,按一下**Add**,然後選擇Add Dynamic NAT Rule選 項以配置動態NAT規則。

Gisco ASDM 6.3 for ASA - 10.77 File View Tools Wizards Window	.241.115 Help
Home Configuration Moni	toring 🔚 Save 🔇 Refresh 🔇 Back 🚫 🏧
Device List 🗗 🖗 🗡	Configuration > Firewall > NAT Rules
🗣 Add <u>î</u> Delete 🚿 Connect	🗣 Add 🗸 🗃 Edit. 🁔 Delete 👌 🗲 🕉 🐚
Firewall 🗇 🕀 🗡	Add Static NAT Rule
Firewal	Add Dynamic NAT Rule
6-3 · · · · ·	Add NAT Exempt Rule
Remote Access VPN	Add Static Policy NAT Rule
Site-to-Site VPN	Add Dynamic Policy NAT Rule
D IPS	1nsert
980	ddress
Device Management	
*	

2. 選擇實際主機所連線的介面的名稱。使用Source欄位中的Details按鈕選擇主機/網路的實際 IP地址。

nterface: inside		<u> </u>	
iource:			
ndahad			
elect a glob	al pool for dynamic translat	9R	in the second
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
L0	(inbound)	Same as original address (identity)	

3. 在本示例中,已選擇整個內部網路。按一下OK以完成選擇。

Mana		TO Address	Haberrah	Description	ohuana
Name	labuark Ohie	IP Address	Netmask	Description	Object NA
E IPYT K	anv	0.0.0.0	0.0.0.0		
	inside-n	172.16.11.0	255.255.255.0		
	manage	10.77.241.64	255.255.255.192		
	outside	209.165.200.0	255.255.255.224		
	20.1.1.10	20.1.1.10	255.255.255.255		
-8	172.16	172.16.11.1	255.255.255.255		
-8	172.16	172.16.11.10	255.255.255.255		
- 3	172.16	172.16.12.2	255.255.255.255		
	209.16	209.165.200.10	255.255.255.255		

4. 按一下Manage以選擇實際網路將對映到的IP地址池。

iterrace:	IINAG		
ource:	nside-network/24		
nslated —			
elect a glob	al pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	6
			Manage
			<u> </u>
nnertion	Settings		

5. 按一下Add以開啟Add Global Address Pool視窗。

Pool ID	Interface	Addresses Pool	

6. 選擇**Range**選項並指定Starting and Ending IP Addresses以及輸出介面。此外,請指定唯一池 ID並按一下Add以將其新增到地址池。按一下OK以返回到「管理全域性池」視窗。

nterface:	outside		~		
Pool ID:	10				
IP Addre	esses to Add				Addresses Pool
Rang	ge	2			<b>11</b> 209.165.200.20 - 209.165.200.40
Starti	ng IP Address:	209.165.200.20			
Endin	g IP Address:	209.165.200.40			
Netm	ask (optional):	255.255.255.192		Add >>	
O Port	Address Transi	lation (PAT)	ſ	<< Delete	
IP Ad	dress:				
Netm	ask (optional):				
O Port Addr	Address Trans ress of the inte	lation (PAT) using IP rface			

7. 按一下**OK**以返回到Add Dynamic NAT Rule視窗。

0110	Interface	Addresses Pool
10	outside	209.165.200.20 - 209.165.200.40
-		

8. 按一下OK以完成動態NAT規則配置。

ource:	inside-network/24				
nslated —					
elect a glo	bal pool for dynamic translat	ion,			
Pool ID	Interface	Addresses Pool			
-0	(outbound)	Same as original address (identity)			
-0	(inbound)	Same as original address (identity)			
10	outside	209.165.200.20 · 209.165.200.40	Manag		

9. 按一下Apply以使更改生效。注意: Enable traffic through the firewall without address translation **選項處於未選中**狀態。

	Time	Original			Translated		
•	Type	Source	Destination	Service	Interface	Address	Service
🗄 inside							
	Dynamic	inside-network/24			outside	209.165.200.20 - 209.165.200.40	
· · ·							

這是此ASDM配置的等效的CLI輸出:

nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0

根據此配置,172.16.11.0網路中的主機將轉換為NAT池209.165.200.20-209.165.200.40中的任何 IP地址。在這裡,NAT池ID非常重要。可以將相同的NAT池分配給另一個內部/dmz網路。如果對映 池的地址少於實際組,則當流量大於預期時,地址可能會用盡。因此,您可以嘗試實施PAT,也可 以嘗試編輯現有地址池以對其進行擴展。

**注意:**在對現有轉換規則進行任何修改時,請注意,需要使用<u>clear xlate</u>命令才能使這些修改生效。 否則,先前的現有連線將保留在連線表中,直到它們超時。使用clear xlate命令時要小心,因為它會 立即終止現有連線。

<u>允許內部主機通過PAT訪問外部網路</u>

如果希望內部主機共用一個公共地址進行轉換,請使用PAT。如果**global**語句指定一個地址,則該 地址為埠轉換。ASA允許每個介面進行一個埠轉換,該轉換支援最多65,535個活動**xlate對**象到單個 全域性地址。

完成以下步驟,以允許內部主機使用PAT訪問外部網路:

1. 轉至Configuration > Firewall > NAT Rules,按一下Add,然後選擇Add Dynamic NAT Rule選

1	Add Static NAT Rule	
R	Add Dynamic NAT Rule	
1	Add NAT Exempt Rule	
3	Add Static Policy NAT Rule	
B	Add Dynamic Policy NAT Rule	
-	Insert	
Į.	Insert After	4

項以配置動態NAT規則。

2. 選擇實際主機所連線的介面的名稱。使用Source欄位中的Details按鈕選擇主機/網路的實際 IP地址,<u>然後選擇inside-network。按一下「Manage」</u>以定義「Translated」位址資訊。

terrace.	inside	·····	
urce:	inside-network/24		
slated			
lect a glob	al pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
-0	(inbound)	Same as original address (identity)	
			Manage

obal Pool		
Edit 懫 Delete		
Interface	Addresses Pool	
(		_
	Cdit The Delete	Cdit The Delete Interface Addresses Pool OK Cancel Help

- 3. 按一下「Add」。
- 4. 選擇Port Address Translation(PAT)using IP address of the interface選項,然後按一下Add將 其新增到地址池。不要忘記為此NAT地址池分配唯一ID。

Interface:	outside	*			
Pool ID:	20				
IP Addr	esses to Add ge		ſ	Addresses Pool	
Start	ing IP Address:				
Endir	ig IP Address:				
Netm	ask (optional):		Add >>		
O Port	Address Translation (PAT	)	<< Delete	2	
IP Ac	idress:		1	t.	
Netm	ask (optional):	-			
Port	Address Translation (PAT	) using IP			
Add	ress of the interface				
	( <b>—</b>				

5. 此處顯示的是已配置的地址池,外部介面是該池中唯一可用的地址。按一下**OK**以返回到Add Dynamic NAT Rule視窗。

20 outside	e autside			
	K Cancel	Help	1	
			,	
─下「 <b>OK</b> 」(確定)。				
Add Dynamic NAT Rule				
riginal				
Interface: inside		×		
Source: inside-network/24		<u></u>		
ranslated				
	ic translation			
Select a global pool for dynam	ic cransiduuri.			
Select a global pool for dynam Pool ID Interface	Addres	ses Pool		
Select a global pool for dynam Pool ID Interface 0 (outbound)	Addres	ses Pool original address (ider	ntity)	
Select a global pool for dynam Pool ID Interface 0 (outbound) 0 (inbound)	Addres Same as Same as	ses Pool original address (ider original address (ider	ntity) ntity)	Mana
Select a global pool for dynam Pool ID Interface 0 (outbound) 0 (inbound) 20 outside	Addres Same as Same as	ses Pool original address (ider original address (ider de	ntity) ntity)	Manag

7. 此處的Configuration > Firewall > NAT Rules窗格中顯示了配置的動態NAT規則。

	Туре	Original	Translated			
		Source	Destination	Service	Interface	Address
inside	9					
1	Dynamic	inside-network/24			outside	outside
		LEK.				
Enab	le traffic through t	be firewall without address t	randation			

這是此PAT配置的等效的CLI輸出:

global (outside) 20 interface nat (inside) 20 172.16.11.0 255.255.255.0

### 限制內部主機訪問外部網路

如果未定義訪問規則,則來自較高安全介面的使用者可以訪問與較低安全介面關聯的任何資源。要 限制特定使用者訪問某些資源,請在ASDM中使用訪問規則。本示例說明如何允許單個使用者訪問 外部資源(使用FTP、SMTP、POP3、HTTPS和WWW)並限制所有其他使用者訪問外部資源。

**注意**:每個訪問清單的結尾都有一個「隱式拒絕」規則。

請完成以下步驟:

1. 轉至Configuration > Firewall > Access Rules,按一下Add,然後選擇Add Access Rule選項以

	dd - 🗹 Edit 📕 Delete 🕈	+
+	Add Access Rule	
+	Add IPv6 Access Rule	
*	Insert	
÷	Insert After	es)
1	any	

建立新的訪問清單條目。

2. 在**Source**欄位中選擇要允許的源IP地址。選擇**any**作為Destination(目標)、**inside**作為 Interface(介面),然後選擇**Permit**(操作)。最後,按一下Service欄位中的**Details**按鈕,為

	🕼 Add Acc	cess Rule		
	Interface: Action: ()	inside 💌 Permit 🔿 Deny		
	Source:	172.16.10.100		
	Destination	any		
	Service:	ip		
	Description:			
	Enable L	ogging Level: Default		
	More Opt	ions		
<b>武電塘建立TCD服</b> 教組			OK Cancel	
別需焊建立TCF服務組。		đ	🕯 Browse Service	
			Add      Edt      Delete     Wh      Service Group      TCP Service Group      UDP Service Group      TCP-UDP Service Group      ICMP Group      Protocol Group      L size	rce Po
3. 按一下Add,然後選擇TC	P Service	Group選項。	eigrp eigrp	

4. 輸入此組的名稱。選擇每個所需的埠,然後按一下Add以將其移動到「組中的成員」欄位。

p Name: Permit-172.10.100	)
ription:	
xisting Service/Service Group:	Members in Grou
Name	Name
E TCP Service Groups	too ftp
RDP	
- Predefined	
- 192> aol	
- 10 bgp	
- 100 chargen	
··· 👥 ofs	
to citrix-ica	
- 100> ctiqbe	Add >>
to daytime	<< Remove
102> domain	
techo	
TOP exec	
📷 finger	
🔞 ftp-data	
- 100- gopher	0
1 am 1-000	
reate new member:	
ort/Range:	

5. 您應在右側欄位中看到所有選定的埠。按一下「OK」以完成服務連線埠選取流程。

cription:			
Existing Service/Service Group;			Members in Group:
Name			Name
nfs	~		ftp
- 100 nntp			👘 💯 ftp-data
- 100 pcanywhere-data			http
pim-auto-rp			nttps
100 pop2			pop3
pptp			too smtp
100> rsh			
100> rtsp		Add >>	a second a second a second
100- sip			
😰 sginet		<< Remove	
😳 ssh	1		
- 🚾 sunrpc			
- IO> tacacs			
😰 talk	10		
teinet			
- 19> uucp			
i top whois	~		
Create new member:			

6. 您可以在此處看到已配置的TCP服務組。按一下「**OK**」(確定)。

				B. H. H. B. L.	LOUD T	Des 1 North
Name		Protocol	Source Ports	Destination Ports	ICMP Type	Description
- E	Permit-1	ccp	default (1 SEEDE)	24		
	TSE rtp	ccp	default (1-65535)	21		
	Ttp-data	top	default (1-65555)	20		
	top https://	top	default (1-65535)	442		
H	nccps	top	default (1-65535)	110		
	in pops	top	default (1-65535)	25		
	Sile Sile	top	der aux (1-05555)	2.5		
- Pre	defined	ccb				
6.	TOP: aol	tcp	default (1-65535)	5190		
1	to bap	tcp	default (1-65535)	179		
	102- chargen	tcp	default (1-65535)	19		
	100 cifs	tcp	default (1-65535)	3020		
	10 citrix-ica	tcp	default (1-65535)	1494		
1.0	100 ctiqbe	tcp	default (1-65535)	2748		
-	100 daytime	tcp	default (1-65535)	13		
-	10 discard	tcp	default (1-65535)	9		
-	100- domain	tcp	default (1-65535)	53		
-	10 echo	tcp	default (1-65535)	7		
-	10 exec	tcp	default (1-65535)	512		
electe	d Service					
Ciocce						

Interface:	inside 💌
Action: 💿	Permit O Deny
Source:	172.16.10.100
Destination	any 🕢
Service:	Permit-172.16.10.100
Description:	
🕑 Enable L	ogging
Logging	Level: Default 😪
More Opt	ions

- 7. 按一下OK以完成設定。
- 8. 在Configuration > Firewall > Access Rules窗格的inside介面下可以看到已配置的訪問規則。

Co	nfigur	ation > Fire	wall > Access Rules							
[	🗣 Add	• 🖉 Edit	🗊 Delete   🛧 🦆 🌡	🖌 🗈 🏥 - 🛛 Q. Find 🖭	Diagram	Export	- 😚 Clear	Hits 🗐	Show Log 🔍	Pa
	#	Enabled Source		Destination	Service		Action	Hits	Logging	Ti
6	a 🚚 ir	nside (2 incom	ing rules)							
	1	<b>~</b>	172.16.10.100	🕫 any	300 Pern	nit-172.1	🖌 Permit		- Americanity	
	2	1	🏟 any	any	IP ip	TCP Gro	TCP Group: Permit-172.16.10.100 TCP: ftp (21)			
10	i 🥵 i	nside IPv6 (2	implicit incoming rules)			TCP: ftp				
	1		🏟 any	Any less secure ne	IP- IP	TCP: ftp-data (20)				
	2		🏟 any	any	IP ip	TCP: https (443)			1.000	
5	5 🔊 n	nanage (2 imp	licit incoming rules)			TCP: pop	3 (110)			
	1		🏟 any	Any less secure ne	IP ip	TCP: sm	tp (25)			

9. 為便於使用,您還可以直接在**Services**頁籤的右側窗格中編輯TCP服務組。按一下**Edit**以直接 修改此服務組。

> Fin	ewall > Access Rules								Addresses Services Time Ranges	
Edit	1 Delete + 4 X	1 1 1 - Q. Find E	Diagram Chapter	- 🔗 Clear	HRs 🖽	Show Log	Packet	Trace	Services di 4	×
abled	Source	Destination	Service	Action	Hits	Logging	Time	Description	Add - Edt To Delete Q Where	Lised
(2 incor	ning rules)								Filter	deat
	172.16.10.100	d any	30 Permit-172.1	🥜 Pernit	a second	Language	1 Corners		Name	1
	any	any	.æ∕ip	O Deny	1000	1.000		Implicit rule	S-TCP Service Groups	-
Pv6 (2	implicit incoming rules)								🖬 📅 Permt-172.16.10.100	
	any	Any less secure ne	.m. ip	🖌 Pernit				Implicit rule: Per	- Mr Rp	
	any	any	a ip	() Deny				Implicit rule	- see Rp-data	
je (2 im	plicit incoming rules)								- me http	
	any	Any less secure ne	je ip	🖌 Pernit				Implicit rule: Per	- 🐲 https	
	any	any	ze ip	O Deny				Implicit rule		
is IPv6	(2 implicit incoming rules)								- Mar smtp	
	any	Any less secure ne	18 ip	🖌 Pernit				Implicit rule: Per	B TRI RDP	
	any	any	je ip	C Deny				Implicit rule	Predefined	
s (2 inc	oming rules)								ter ad	
	20.1.1.10	A 209.165.200.10	ROP	🖌 Permit	(	D		A Statement of a	mg/ bgp	
	any any	any 🔅	JE ip	O Deny				Implicit rule	- BB chargen	

10. 它會再次重定向到「編輯TCP服務組」視窗。根據您的要求執行修改,然後按一下**OK**以儲存 更改。

kisting Service/Service Group:		Members in Group:
Name		Name
-TCP Service Groups	~	r-100 ftp
RDP		100 ftp-data
Predefined		- tet http
- 10> aol		- 100> https
- 😰 bgp	=	ree pop3
- 😥 chargen		smtp
😰 cifs		
- 10> citrix-ica		
- 102> ctiqbe	Add	>>
- 😥 daytime	<< Re	move
👓 😥 discard	· · · · · · · · · · · · · · · · · · ·	
- 😎 domain		
- 19 echo		
exec		
- 100> finger		
102> gopher		
- 102/ h323		
an hashesses		

11. 此處顯示了ASDM的完整檢視

						£000.POF			
Save @	Reliesh 🔇 Back 🤅	Denne 9 Hub							CISCO
Nauration > Fir	weall > Access Rules						-	Addresses Services	Time Ranges
ANI - E Edk	Dente + 4	K Ball - Q mil E	Dagan Gitoor	· () Char His	() Show Log	Packet Trace		Services	d' 0 ×
Enabled	Source	Destination	Service	Action Hit	s Logging	Time Description	n	AN - B ER Des	e Q Where Use
🗯 inside (2 incor	ning rules)		-				-	Fiker:	(HeriCle
2	172-16-10.000	CO BY	SP Ferstel 172.1.	Denv	NUS CHENNER	Indet rule		Name	
Pinenage (2 im	plicit incoming rules)							E Perch-172.16.10.1	00
1	any any	Any less secure ne	20	🖋 Pomt		Depkit rule	(Free	- 100 Rp	
							×.	- sa ftp-data	
ess Pule Type 🔘	Pri and PV6 @ Pvi	Only O IPv6 Only						- 500 Hitp - 100 Hitps	
	Add - C tok Crusted Inside (2 inca Inside (2 inca)) Inside (2 inca Inside (2 inca)) Inside (2 inca)) Inside (2 inca)) Inside (2 inca)) Inside (2 inca)) Insi	Save Q Policish Q Back     Save Q Policish Q Back     Add = @ Edit D Takite + 4     Enabled Source     Ministe (2 Incoming rules)     Policis Policis (2 Incoming rules)     Q any     Ministry (2 Incoming rules)     I Q any      this Policis Type Q IPoli and IPV6 Q IPoli	Save Carbon Tarken Tark Heb  Save Carbon Sources Roles  Add - Carbon Sources Roles  Add - Carbon Sources  Add - Carbon Sources  Tarbon Source	Save Q Torken Q Tool Q T	Save Q Formed > Access Sules     Add = @ Eds. @ Texture + 4	Save Q = Indivent     If Back     If Help       Intersation > Forewall > Access Roles       Add + Q = Edx     Delate     If Date       F     Enabled     Source     Destination       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       Image: Q = Indivent of Date     If Date     If Date       If Date     If Date	Save Q Profesh     Task     Y Heb       disarution > Finnesdi > Access Roles       Add + G Edx     Delse + 4     B B     Q Find B Delses       Finded Source     Destination     Service     Action     Hits     Service Packet Trace       Profile (2 incoming rules)     B MY     Service     Action     Hits     Logging     Time Description       Profile (2 incoming rules)     B MY     Service     Action     Hits     Logging     Time Description       2     G MY     Service     Service     Action     Hits     Logging     Time Description       2     G MY     Service     Service     Service     Direct Hits     Mediation       2     G MY     G My     Service (2 incoming rules)     Mediation     Service (2 incoming rules)     Mediation       2     G MY     G My Hey (2 incoming rules)     G My Hey (2 incoming rules)     Direct Hits     Direct Hits       3     May (2 incoming rules)     G My Hey (2 incoming rules)     Mediation     Mediation     Mediation       2     G My     My Hey (2 incoming rules)     Mediation     Mediation     Mediation       3     May (2 incoming rules)     Mediation     Mediation     Mediation       3     May (2 incoming rules)     Mediation     <	Save Q Torken Q Tool ()     Save Q Torken Q Tool ()	Save Q a notivelit Q Back       Q Hole         dissuration > fixmedit > Access Rodes       Addresses         Add - Q Edit Q Delate + 4       B Q Q Find B Delayan D Deport + 1 Course Q Packet Trace         Add - Q Edit Q Delate + 4       B Q Q Find B Delayan D Deport + 1 Course Q Q Packet Trace         P Ended Source       Destination         P Ended Source       Destination         P Ended Source       Destination         P Ended Source       Destination         P Ended C Decoming rules)       Provide State         P Ender (2 insplict Incoming rules)       Provide State         Q marks       Provide State         Q marks

這是等效的CLI配置:

.

object-group service Permit-172.16.10.100 TCP port-object eq ftp port-object eq ftp-data port-object eq www port-object eq https port-object eq pop3 port-object eq smtp ! access-list inside\_access\_in extended permit TCP host 172.16.10.100 any object-group Permit-172.16.10.100 ! access-group inside\_access\_in in interface inside ! 有關實施訪問控制的完整資訊,請參閱<u>通過ASDM GUI新增或修改訪問清單</u>。

# 

本節介紹如何在具有相同安全級別的介面內啟用流量。

以下說明介紹了如何啟用介面內通訊。

這對於進入介面但隨後從同一介面路由出去的VPN流量很有用。在此案例中,VPN流量可能未加密 ,或者可能針對另一個VPN連線重新加密。前往Configuration > Device Setup > Interfaces,然後 選擇Enable traffic between two or more hosts connected to the same interface選項。

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redun
Ethernet0/0	outside	Yes	0	209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	100	172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	90	10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No
<						
Enable traffic betw	een two or more inter een two or more host	faces which a s connected t	re configured o	with same security le	Annly Res	et )

以下說明介紹了如何啟用介面間通訊。

這對於允許具有同等安全級別的介面之間的通訊非常有用。前往Configuration > Device Setup > Interfaces,然後選擇Enable traffic between two or more interfaces that configured with same security levels選項。

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redur
Ethernet0/0	outside	Yes	0	209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	100	172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	90	10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No
<			<u>ilu</u>			
🔽 Enable traffic betw	een two or more inter	faces which a	re configured (	with same security le	vels	
Enable traffic betw	een two or more host	s connected t	o the same inte	erface		
Linable traffic betw						

這是這兩個設定的等效CLI:

same-security-traffic permit intra-interface
same-security-traffic permit inter-interface

## <u> 允許不受信任的主機訪問受信任網路中的主機</u>

這可以通過應用靜態NAT轉換和允許這些主機的訪問規則來實現。每當外部使用者想要訪問位於內 部網路中的任何伺服器時,都需要進行此配置。內部網路中的伺服器將具有不可在Internet上路由的 專用IP地址。因此,您需要通過靜態NAT規則將該私有IP地址轉換為公有IP地址。假設您有一個內 部伺服器(172.16.11.5)。為了讓此功能正常工作,您需要將此專用伺服器IP轉換為公共IP。本示例 說明如何實施雙向靜態NAT以將172.16.11.5轉換為209.165.200.5。

此處未顯示有關通過實施訪問規則允許外部使用者訪問此Web伺服器的部分。為了便於理解,此處 將顯示一個簡短的CLI片段:

access-list 101 permit TCP any host 209.165.200.5 有關詳細資訊,請參閱通過ASDM GUI新增或修改訪問清單。

**注意:指**定關鍵字「any」允許來自外部世界的任何使用者訪問此伺服器。此外,如果沒有為任何 服務埠指定該埠,則可在任何服務埠保持開啟狀態時訪問伺服器。實作時請務必小心,建議您將此 許可權限製為單個外部使用者以及伺服器上的所需埠。

完成以下步驟以配置靜態NAT:

1. 轉至Configuration > Firewall > NAT Rules,按一下Add,然後選擇Add Static NAT Rule。



2. 指定原始IP地址、轉換後的IP地址及其相關介面,然後按一下**OK**。

and a second	inside	~
Source:	172.16.11.5	-
ranslated		
Interface:	outside	*
() Use IP Address:	209.165.200.5	-
ort Address Translatio	n (PAT)	
ort Address Translatio	n (PAT) dress Translation (PAT)	
Protocol:	n (PAT) dress Translation (PAT)	
ort Address Translatio     Enable Port Ad     Protocol:     Original Port:	n (PAT) dress Translation (PAT) TCP UDP	
ort Address Translatio Enable Port Ad Protocol: Original Port: Translated Port	n (PAT) dress Translation (PAT) TCP UDP	

3. 您可以在此處看到配置的靜態NAT條目。按一下Apply以將此命令傳送到ASA。

# Tune		Original		Translated		
*	Type	Source	Destination	Service	Interface	Address
insid	le (1 Static rules, 1 l	Dynamic rules)				
1	Static	<b>5</b> 172.16.11.5			outside	209.165.200.5
2	Dynamic	inside-network/24	A CONTRACTOR OF A CONTRACTOR O		outside	outside
1						
TEnn	ble traffic through t	he firewall without address t	translation			

以下是此ASDM配置的簡短CLI示例:

! static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255 !

# <u>禁用特定主機/網路的NAT</u>

當需要將特定主機或網路免除NAT時,請新增NAT豁免規則以禁用地址轉換。這樣,轉換後的主機 和遠端主機都可以發起連線。

請完成以下步驟:

1. 轉至Configuration > Firewall > NAT Rules,按一下Add,然後選擇Add NAT Exempt Rule。



2. 這裡,內部網路172.18.10.0已免於地址轉換。確保已選擇Exempt選項。NAT Exempt Direction有兩個選項:到較低安全介面的出站流量到更高安全介面的入站流量預設選項用於出 站流量。按一下「OK」以完成步驟。

📬 Add NAT I	ixempt Rule	
Action:	Exempt     O Do not exempt	
Original		
Interface:	inside 😽	
Source:	172.18.10.0	
Destination:	any	
NAT Exempt Di	rection	
NAT Exe	mpt outbound traffic from interface 'inside' to lower security	
O NAT Exe	mpt inbound traffic from interface 'inside' to higher security	
Description		
	OK Cancel Help	
		<b>注意</b> :選擇Do not exempt <mark>選</mark>

**項**時,該特定主機將不會被免除NAT,並且會使用「deny」關鍵字新增單獨的訪問規則。這有 助於避免特定主機免除NAT,因為除這些主機之外的整個子網將免除NAT。

3. 您可以在此處檢視出站方向的NAT豁免規則。按一下Apply以將配置傳送到ASA。

	Turne	Original		Translated	
	туре	Source	Source Destination		Interface
insid	e (1 Exempt rules, 1	Static rules, 1 Dynamic rul	les)		a statute and
1	😅 Exempt	172.18.10.0	🐔 any		(outbound)
2	1 Static	3 172.16.11.5		-	outside
3	III Dynamic	📸 inside-network/24			outside
1					
Ena	ble traffic through th	e firewall without address	translation		
-					

#### 定供您参考的到寺ULI輛工

access-list inside\_nat0\_outbound extended permit ip host 172.18.10.0 any
!

nat (inside) 0 access-list inside\_nat0\_outbound

4. 在這裡,您可以看到如何編輯NAT豁免規則作為其方向。按一下OK使該選項生效。

	Exempt	🔿 Do not exempt				
Original						
Interface:	inside					
Source:	172.18.10.	0	-			
Destination:	any		-			
NAT Exempt Di	rection					
O NAT Exe	mpt outbour	d traffic from interface 'in	side' to lower secur	ity interfaces (	(default)	
NAT Eve	mot inhound	traffic from interface linci	de' to bigber securi	ty interfaced		
C MAIL EAG	inperindodina	ciance non-incensee insi	de comigner securi	cy incerraces		
Description —						
	C	ОК Саг	ncel Help			
ᆂᄱᆕᆝᆈᆍᇧ			ncel Help			
在您可以看到	到方向已變	OK Car 更為 <i>傳入</i> 。	ncel Help			
在您可以看到 onfiguration	到方向已變 >Firewall	OK Car 更為傳入。 > NAT Rules	ncel Help			
在您可以看到 onfiguration ◆ Add ▼ 2	到方向已變 >Firewall 'Edt	OK Car 更為傳入。 > NAT Rules	ncel Help	🖭 Diagram 🤇	Packet Trace	
在您可以看到 onfiguration 全 Add - 〇	到方向已變 >Firewall 'Edt	OK Car 至為傳入。 > NAT Rules elete	ncel Help	🖭 Diagram 🥰	Packet Trace Translated	
在您可以看到 onfiguration ◆ Add • 図 # Typ	到方向已變 >Firewall Edt îî De	OK Car 更為傳入。 > NAT Rules elete	ncel Help	Diagram 🤇	Packet Trace Translated Interface	
在您可以看到 onfiguration ◆ Add • 図 * Typ 回 inside (1 Exe	到方向已變 >Firewall Edit	OK Car 更為傳入。 > NAT Rules lete	ncel Help	Diagram 🤇	Packet Trace Translated Interface	
在您可以看到 onfiguration ◆ Add ~ 2 * Typ 回 inside (1 Exe 1	到方向已變 > Firewall <sup>2</sup> Edit	OK Car 更為傳入。 > NAT Rules Hete	ncel Help	Diagram C	Packet Trace Translated Interface (inbound)	
在您可以看到 onfiguration ● Add - ② # Typ 回 inside (1 Exe 1 = 1 2 + 1 5	到方向已變 > Firewall Edit 會 De empt rules, 1 Exempt Static	OK Car 空更為傳入。 > NAT Rules Hete	ncel Help	Diagram C	Packet Trace Translated Interface (inbound) outside	
在您可以看到 onfiguration ● Add • ☑ # Typ I inside (1 Exe I I I I 2 I I 3 III I	到方向已變 >Firewall Edit 前 De empt rules, 1 Exempt Static Dynamic	OK Car 更為傳入。 > NAT Rules elete	ncel Help	Diagram C	Packet Trace Translated Interface (inbound) outside outside	

#### 按一下**Apply**以將此CLI輸出傳送到ASA:

access-list inside\_nat0\_outbound extended permit ip host 172.18.10.0 any
!

nat (inside) 0 access-list inside\_nat0\_outbound outside

**注意:**從這裡可以看到,在**nat** 0命令的末尾新增了一個新的關鍵字(outside)。此功能稱為**外部** NAT。

6. 禁用NAT的另一種方法是實施身份NAT。身份NAT將主機轉換為相同的IP地址。以下是常規靜 態身份NAT示例,其中主機(172.16.11.20)在從外部訪問時轉換為同一個IP地址。

📬 Add Static NAT R	ale		
Original			
Interface:	inside	~	
Source:	172.16.11.20	-	
Translated			
Interface:	outside	~	
() Use IP Address:	172.16.11.20		
O Use Interface IP	Address		
Port Address Translation	n (PAT)		
Enable Port Ad	dress Translation (PAT)		
Protocol:	TCP UDP		
Original Port:			
Translated Port			
Connection Setting	5	*	
(C)			
	K Cancel Help		

## <u>連線埠重新導向(轉送)(含靜態)</u>

埠轉發或埠重定向是一項有用的功能,外部使用者可嘗試訪問特定埠上的內部伺服器。為此,內部伺服器(具有私有IP地址)將被轉換為公有IP地址,從而允許特定埠訪問。

在本例中,外部使用者想要訪問埠25上的SMTP伺服器209.165.200.15。這可通過兩個步驟完成:

1. 將埠25上的內部郵件伺服器172.16.11.15轉換為埠25上的公共IP地址209.165.200.15。

2. 允許訪問埠25上的公共郵件伺服器209.165.200.15。

當外部使用者嘗試訪問埠25上的伺服器209.165.200.15時,此流量將重定向到埠25上的內部郵件伺服器172.16.11 15。

1. 轉至Configuration > Firewall > NAT Rules,按一下Add,然後選擇Add Static NAT Rule。



2. 指定原始源、轉換後的IP地址及其相關介面。選擇Enable Port Address Translation(PAT),指 定要重定向的埠,然後按一下OK。

🗯 Add Static NAT R	tule	E
Original	• EP	
Interface:	inside	~
Source:	172.16.11.15	-
Translated		
Interface:	outside	~
💿 Use IP Address:	209.165.200.15	
Port Address Translatio	n (PAT) dress Translation (PAT)	
Protocol:		
Original Port:	25	
Translated Port	: 25	
Connection Setting	5	8
	Cancel Help	

3. 配置的靜態PAT規則如下所示

2

	Tune	Original			Translated		
-	type	Source	Destination	Service	Interface	Address	Servic
1	😅 Exempt	A 172.18.10.0	any		(outbound)		
2	🗐 No Exempt	3 172.20.10.10	any		(outbound)		
3	Static	172.16.11.15		BOD smtp	outside	209.165.200.15	🐨 sm
4	· Static	3 172.16.11.5			outside	209.165.200.5	
3							>

這是等效的CLI輸出:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
255.255.255.255
!
```

4. 以下是允許外部使用者訪問位於209.165.200.15的公共smtp伺服器的訪問規則

				TC TC	P Group: smtp-access P: smtp (25)
3		anv	any		C Denv
2	<b>V</b>	🧐 any	209.165.200.15	smtp-access	; 🖌 🖌 Permit
1		🖳 20.1.1.10	🚇 209.165.200.10	RDP	🖌 Permit
a 🥦 ou	tside (3 inc	oming rules)			
2		🇳 any	🏟 any	IP/ ip	🔇 Deny
1		🧼 any	Any less secure ne	IP IP	V Permit

注意:確保使用特定主機,而不是在訪問規則的源中使用any關鍵字。

# 使用靜態限制TCP/UDP會話

您可以使用靜態規則指定TCP/UDP連線的最大數量。您還可以指定初始連線的最大數量。半開連線 是一種半開狀態的連線。其中大量資料將影響ASA的效能。限制這些連線將在某種程度上防止某些 攻擊,如DoS和SYN。要完全緩解,您需要在MPF框架中定義策略,這超出了本文檔的範圍。有關 此主題的其他資訊,請參閱<u>減輕網路攻擊</u>。

請完成以下步驟:

1. 按一下Connection Settings頁籤,並指定此靜態轉換的最大連線數。

original		
Interface:	inside	
Source:	172.16.11.15	
ranslated		
Interface:	outside	~
💽 Use IP Address:	209.165.200.15	
O Use Interface IP /	iddress	
ort Address Translation	(PAT)	
Enable Port Add	iress Translation (PAT)	
Protocol:		
Original Port:	smtp	
Translated Port	smtp	
Connection Setting	5	٨
Translate the Df	IS replies that match the translation rule	
Randomize sequ	ence number	
Maximum TCP Conne	actions: 100	
Maximum UDP Conn	ections: 0	
Maximum Embryonic	Connections: 50	
~		

2. 這些影象顯示了此特定靜態轉換的連線限制

🕏 Add 🗕 🧭 Edit 📋	Delete 🛧 🗲	* 🖻 🛍 -	🔍 Find 🖭 Di	agram 🏹 Packet Trace	
Original			Translated		
Source	Destination	Service	Interface	Address	Service
tatic rules, 1 Dynamic r	ules)				
172.18.10.0	any		(outbound)		
172.20.10.10	any		(outbound)		
172.16.11.15		😥 smtp	outside	209.165.200.15	tto smtp

Options				
DNS Rewrite	Max TCP Connections	Embryonic Limit	Max UDP Connections	Randomize Seque
	100	50	Unlimited	
				And the second se

這是等效的CLI輸出:

static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255 TCP 100 50

## <u>時間型存取清單</u>

1

!

本節介紹如何使用ASDM實施基於時間的訪問清單。可以基於時間應用訪問規則。為了實施此功能 ,您需要定義一個時間範圍,指定按天/周/月/年計時。然後,您需要將此時間範圍繫結到所需的訪 問規則。時間範圍可通過兩種方式定義:

1. 絕對 — 定義包含開始時間和結束時間的時間段。

2. 定期 — 也稱為定期。定義以指定間隔發生的時間段。

**注意:**在配置時間範圍之前,請確保已為ASA配置了正確的日期/時間設定,因為此功能使用系統時 鐘設定實施。使ASA與NTP伺服器同步將產生更好的結果。

完成以下步驟,以便通過ASDM配置此功能:

1. 定義訪問規則時,按一下Time Range欄位中的Details按鈕。

Add Acc	ess Rule
Interface:	inside 💌
Action: OI	Permit 💿 Deny
Source:	172.16.10.50
Destination	any 🔄
Service:	ip 🔄
Description:	
🕑 Enable L	ogging
Logging I	evel: Default 💌
More Opt	ons
Enable	Rule
Traffic Dire	ction: 🔿 In 💿 Out
Source Ser	vice: (TCP or L
Logging In	erval: 300 seconds
Time Rang	*
	OK Cancel Help
	📓 Browse Time Range
	Add Edit To Delete

3. 定義時間範圍的名稱,並指定開始時間和結束時間。按一下「OK」(確定)。

Time Range Name: Restrict-Usage							
Start Time		End Time					
O Start now		O Never e	end				
<ul> <li>Start at</li> </ul>		💽 End at :	(inclusive)				
Month: February 💉 Day: 05 🛐	Year: 2011 🛩	Month:	February 💌	Day:	06 🛩	Year:	2011
Hour: 14 Minute: 00 N	8	Hour:	16 💌	Minute:	30 💌		
You can further constrain the active time of t	his range by specifying r	recurring ranges.	The recurring tin	e ranges	will be act	tive wit	hin the
						1	Add
							Edit
							Edit Delete
							Edit Delete
							Edit Delete
							Edit Delete
							Edit
		ancel H	lelp				Edit
恐可以在此處檢視時間範圍。按·		ncel H Ē <sup>[</sup> Add Act	cess Rule	視窗。	,		Edit Delete
S可以在此處檢視時間範圍。按 ■ Browse Time Range	⊂а	ncel H Ē <sup>Γ</sup> Add Act	œÞ cess Rule⊥	視窗。	,		Edit Delete
怒可以在此處檢視時間範圍。按 <mark>쥷 Browse Time Range</mark>	○K ○ C ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	ncel H Ē <sup>Γ</sup> Add Aca	op cess Rule 」	視窗。	2		Edit Delete

5.	見在您可以看到Restrict-Usage時間範圍已繫結到此訪問規則	0

Help

Cancel

Res... 14:00 05 Fe... 16:30 06 F...

ſ

OK

📬 Add Acc	ess Rule	
Interface:	inside 💌	
Action: O	Permit 💿 Deny	
Source:	172.16.10.50	
Destination	any 💮	
Service:	ip 🔄	
Description:		
Enable L	ogging .evel: Default	
More Opt	ions	
🔽 Enable	Rule	
Traffic Dire	ection: O In 💿 Out	
Source Ser	vice: (TCP or UDP servi	
Logging In	terval: 300 seconds	
Time Rang	e: Restrict-Usage 💌	
	OK Cancel Help	根據此訪問規則配

置,位於172.16.10.50的使用者被限制使用從2011年2月5日下午2點到2011年2月6日下午 4.30點之間的任何資源。這是等效的CLI輸出:

time-range Restrict-Usage	
absolute start 14:00 05 February 2011 end 16:30 06 Feb	oruary 2011
1	
access-list inside_access_out extended deny ip host 172	2.16.10.50 any
time-range Restrict-Usage	
!	
access-group inside_access_out in interface inside	

6. 以下示例說明如何指定循環時間範圍。按一下Add以定義定期時間範圍。

fime Range Name: Restrict-Usage	1		
Start Time		End Time	
⊖ Start now		O Never end	
⊙ Start at		End at (inclusive)	
Month: February 🖌 Da	ay: 05 💙 Year: 2011 💙	Month: March	Day: 06 💙 Year: 20
Hour: 00 Mi	inute: 00 ⊻	Hour: 00	Minute: 30 💌
Recurring Time Ranges			
You can further constrain the act start and stop time specified.	tive time of this range by specifying	g recurring ranges. The recurring bi	me ranges will be active within the
			Add
			Edi
			[ min
· 據您的要求指定設定, ———————————————————————————————————	,然後按一下OK完成。		-
🕻 Add Recurring Time	Range		
Specify days of the wee	k and times on which this rec	urring range will be active	
Ecr evende une this or	ation when you want the time	range to be active every	
Monday through Thursd	lay, from 8:00 through 16:59	, only.	
Days of the Week			
O Every day			
~			
🔿 Weekdays			
<ul> <li>Weekdays</li> <li>Weekends</li> </ul>			
<ul> <li>Weekdays</li> <li>Weekends</li> <li>On these days of</li> </ul>	of the week:		
<ul> <li>Weekdays</li> <li>Weekends</li> <li>On these days of Mon I Tu</li> </ul>	of the week: ue 🔽 Wed 🔽 Thu 📿 f	≂ri []Sat []Sun	
<ul> <li>○ Weekdays</li> <li>○ Weekends</li> <li>⊙ On these days o</li> <li>✓ Mon ✓ Tu</li> <li>Daily Start Time</li> </ul>	of the week: ue ved ved thu v f Daily E	⁼ri □ Sat □ Sun ind Time (Inclusive)	
<ul> <li>○ Weekdays</li> <li>○ Weekends</li> <li>⊙ On these days o</li> <li>✓ Mon ✓ Tu</li> <li>Daily Start Time</li> <li>Hour 15 ✓ Minu</li> </ul>	of the week: ue ved ved thu v f Daily E ute 00 ved Hour	Tri Sat Sun Ind Time (Inclusive)	
<ul> <li>○ Weekdays</li> <li>○ Weekends</li> <li>⊙ On these days o</li> <li>☑ Mon ☑ Tu</li> <li>Daily Start Time</li> <li>Hour 15 ☑ Minu</li> </ul>	of the week: ue ved v Thu v f ute 00 v	Fri 🔲 Sat 🛄 Sun Ind Time (Inclusive) I 🔯 💉 Minute 00 💉	
<ul> <li>○ Weekdays</li> <li>○ Weekends</li> <li>○ On these days of</li> <li>✓ Mon ✓ Tu</li> <li>Daily Start Time</li> <li>Hour 15 ✓ Minu</li> <li>○ Specify a weekly interval</li> </ul>	of the week: ue ved ved thu v f ute 00 ved Hour al when this recurring range v	Fri Sat Sun Ind Time (Inclusive) Ind Time (Inclusive) Ind Time (Or Inclusive)	
<ul> <li>♦ Weekdays</li> <li>♦ Weekends</li> <li>♦ On these days of</li> <li>♥ Mon</li> <li>♥ Tu</li> <li>Daily Start Time</li> <li>Hour</li> <li>15</li> <li>♥ Minu</li> <li>♦ Specify a weekly intervation</li> <li>For example, use this op</li> </ul>	of the week: ue ved ved thu ver ute 00 ver al when this recurring range ve ption when you want the time	Fri Sat Sun End Time (Inclusive) Minute 00 will be active a range to be active	
<ul> <li>♦ Weekdays</li> <li>♦ Weekends</li> <li>♦ On these days of</li> <li>♥ Mon</li> <li>♥ Mon</li> <li>♥ Tu</li> <li>Daily Start Time</li> <li>Hour</li> <li>15</li> <li>♥ Minu</li> <li>Specify a weekly interval</li> <li>For example, use this op continuously from Monda</li> </ul>	of the week: ue veek: ute 00 ved verthu vert ute 00 verthe Hour al when this recurring range ve ption when you want the time ay at 8:00 through Friday at	Fri       Sat       Sun         Ind Time (Inclusive)         Image (Inclu	
<ul> <li>♦ Weekdays</li> <li>♦ Weekends</li> <li>♦ On these days of</li> <li>♥ Mon</li> <li>♥ Tu</li> <li>Daily Start Time</li> <li>Hour</li> <li>15</li> <li>Minu</li> <li>Specify a weekly interval</li> <li>For example, use this op continuously from Monda</li> <li>Weekly Interval</li> </ul>	of the week: ue veek: ute veek veek to the veek ute veek ute veek ute veek ute veek veek ute veek veek veek veek veek veek veek vee	TI Sat Sun and Time (Inclusive) Minute 00 will be active a range to be active 16:59.	
<ul> <li>○ Weekdays</li> <li>○ Weekends</li> <li>○ On these days of</li> <li>☑ Mon ☑ Tu</li> <li>Daily Start Time</li> <li>Hour 15 ☑ Minu</li> <li>○ Specify a weekly interval</li> <li>For example, use this op continuously from Monday</li> <li>Weekly Interval</li> <li>From: Monday</li> </ul>	of the week: ue veek: ue veek: ue veek: Daily E Hour al when this recurring range we ption when you want the time ay at 8:00 through Friday at veek: Hour: 00 veek: Hour: 00 veek:	Fri       Sat       Sun         and Time (Inclusive)       Inclusive)         Image of the sective       Image of the sective         ange to be active       Image of the sective         16:59.       Image of the sective	

8. 按一下**OK**以返回到「時間範圍」視窗。

as kant fime	e Range													
Time Range N	ame: Restri	ict-Us	age											
Start Time —							End Time							
🔘 Start no							O Never e	end						
<ul> <li>Start at</li> </ul>							• End at	(inclusive)						
Month:	February	~	Day:	05 🛩	Year:	2011 💌	Month:	March	~	Day:	06	~	Year:	201
Hour:	00	Y	Minute:	00 🗸			Hour:	00	~	Minute:	30	~		
start and st weekdays	op time spe 15:00 throu	ofied. gh 20	:00											Add
														Ed≹
														Delet
1													4	
				d	0									

根據此配置,從172.16.10.50上的使用者被拒絕在除星期六和星期日外的所有工作日(從下午 3點到晚上8點)訪問任何資源。

```
!
time-range Restrict-Usage
absolute start 00:00 05 February 2011 end 00:30 06 March 2011
periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

**註:如果time-range**命令同時指定了絕對值和週期值,則只有在達到絕對開始時間後才會評估 periodic命令,而在達到絕對結束時間後不會進一步評估。

# 相關資訊

- <u>Cisco ASA文檔頁面</u>
- 技術支援與文件 Cisco Systems